

## HIE Task Force – Legal/Policy Workgroup

### Table of Issues for Privacy and Security Framework

Issue	Recommended Resolution	Interested Parties	Process for Resolution	Public Policy Considerations
				In general: <ul style="list-style-type: none"> <li>• Patient privacy</li> <li>• Public health</li> <li>• Quality improvement</li> <li>• Compliance</li> <li>• Liability</li> </ul>
<b>Individual Access</b>				
Who can access HIE, what can they access, and under what circumstances	<ul style="list-style-type: none"> <li>• Specifically address in health care provider licensing statutes or address generally in enabling legislation</li> <li>• See BTO proposal</li> </ul>			
<b>Correction</b>				
Corrections to Information <ul style="list-style-type: none"> <li>• Define process for correcting information</li> <li>• What warrants correction?</li> <li>• Who decides if correction is appropriate?</li> <li>• What if there's disagreement about correction?</li> <li>• Who makes correction?</li> <li>• When is correction made? Should there be time frames?</li> <li>• Is there a responsibility to</li> </ul>	<ul style="list-style-type: none"> <li>• Need state legislation (should probably be part of enabling legislation)</li> </ul>			

<p>correct? If so, who has it?</p> <ul style="list-style-type: none"> <li>Who is liable for damage if treatment is rendered based on incorrect information?</li> </ul>				
<b>Openness and Transparency</b>				
<ul style="list-style-type: none"> <li>Proposed governance includes broad community representation</li> <li>Strong educational component proposed</li> <li>Regular reports to the public</li> <li>Application of FOIA and APA to policy setting processes</li> </ul>	Content elements could be defined in state law (see NM)			
<b>Individual Choice</b>				
<p>Patient Consent</p> <ul style="list-style-type: none"> <li>Opt-in/Opt-Out</li> <li>ID situations when patient consent not required – ER, public health reporting, law enforcement</li> <li>Accounting of disclosure of electronic information (also see</li> </ul>	<ul style="list-style-type: none"> <li>Need state legislation</li> <li>Most states doing opt-out (sfi: check /NCSL)</li> <li>Need to consider how forms impact policy considerations</li> <li>Article on CA HIEs folding</li> </ul>			Encourage greater participation in HIE as opposed to higher level of transparency & openness

<p>patient/provider notice below)</p> <ul style="list-style-type: none"> <li>Breach notification</li> </ul>				
<p>Patient access to information</p> <ul style="list-style-type: none"> <li>Should there be situations in which patient should not have access?</li> </ul>				
<b>Collection, Use and Disclosure Limitations</b>				
<p>Original record will be the electronic file – no paper copy or printout.</p>	<p>What are the implications of this change?</p> <p>Will the transformation to an electronic system impact ownership. For example, if ownership of data is linked to a single provider entry as opposed to how will the HIE change</p> <p>All info re one patient</p> <p>Compilations of info across patient files</p>			
<p>Ownership of Information</p>	<p>Resolving this issue may not be an initial barrier to implementation of HIE but will ultimately require resolution at state level where property rights are generally determined. A legislative approach may provide greater control over the policy choices as opposed to leaving the issue for judicial resolution. (Note: Issue has been discussed extensively at federal level w/o consensus on resolution.)</p>			

<p>Use of Data</p> <ul style="list-style-type: none"> <li>• Define the contents of the HIE</li> <li>• Will it include results of tests administered by non-health entities, such as law enforcement, schools or employers</li> <li>• Define scope or levels of availability</li> <li>• Determine who has access to what</li> <li>• Distinction between viewable information and downloadable information</li> <li>• Implement higher protections for info re abuse reporting, drug, HIV, psych issues</li> <li>• To identify pre-existing conditions</li> <li>• To deny claims</li> <li>• To deny coverage</li> <li>• To make employment decisions</li> <li>• To make law enforcement decisions</li> <li>• To support regulatory actions</li> <li>• To identify cost centers for business development</li> </ul>	<ul style="list-style-type: none"> <li>• Need state legislation (should probably be part of enabling legislation)</li> </ul>			
<p>Interface with Medicaid</p> <ul style="list-style-type: none"> <li>• MMIS capabilities</li> <li>• Electronic signatures</li> </ul>				
Interface with Medicare and				

other federal programs				
Notice to patient <ul style="list-style-type: none"> <li>• When information accessed</li> <li>• When information that identifies patient is accessed</li> <li>• When de-identified information is accessed</li> <li>• Breach notification</li> <li>• What if abuse reporting is involved</li> <li>• What if fraud is alleged</li> </ul>	Need state legislation (should probably be part of enabling legislation)			
Notice to provider				
Application of FOIA				
Court Processes <ul style="list-style-type: none"> <li>• Rules of Discovery</li> <li>• Rules of Evidence</li> </ul>		AR Supreme Court Ark Bar Association Trial Lawyers Association Tort Reform Advocates	Changes in Rules of Evidence and other court procedures are addressed through the AR Supreme Court	
Subpoenas <ul style="list-style-type: none"> <li>• Court issued</li> <li>• Agency issued</li> <li>• Legislature issued</li> </ul>				
<b>Data Quality and Integrity</b>				
Independent audits				
Process for correction				
<b>Safeguards</b>				
Administrative security	<ul style="list-style-type: none"> <li>• Who or what office is responsible</li> </ul>			
Technical security	<ul style="list-style-type: none"> <li>• Who or what office is responsible</li> </ul>			

Physical security	<ul style="list-style-type: none"> <li>Who or what office is responsible</li> </ul>			
Audit process: -Data access -Compliance				
Possible application of FISMA				
Immunity from liability under certain circumstances	<ul style="list-style-type: none"> <li>Need to define parameters of immunity in state law</li> </ul>			
<b>Accountability</b>				
Governance  -Role of agency in terms of regulatory oversight and compliance with current privacy laws (physical access, technical access, and administrative controls)? Review of other agencies, providers, privacy entities? -Is agency a business associate? -Mandatory/permissive participation of providers? -Will there be a fee structure? If so, who will pay? -What technical stnds will be applied? (address in regulations & contracts) -What entity will be responsible for completing reporting requirements? -What entity will be responsible for auditing HIE	<ul style="list-style-type: none"> <li>Need state enabling legislation</li> <li>Need state appropriation with funding</li> </ul>			

system for security?				
<p>Contract Issues</p> <ul style="list-style-type: none"> <li>• State Vendor Agreement</li> <li>• Subscription/Trust Agreements</li> <li>• Business Associate Agreements</li> <li>• Data Use Agreements</li> <li>• Data Sharing Agreements</li> <li>• Reciprocal Support Agreements</li> </ul>	<ul style="list-style-type: none"> <li>• Need to engage experienced IT contract lawyers</li> <li>• All contracts must address legal and contractual penalties for noncompliance, nonperformance, and improper access to or release of data and information</li> </ul>			
<p>Unauthorized access to system</p> <p>Down-line release information from system – legal access, then inappropriate release of results obtained</p>	<ul style="list-style-type: none"> <li>• Need state laws to establish civil and criminal penalties</li> </ul>			
<p>Identify entities responsible for enforcement and define scope of authority</p> <ul style="list-style-type: none"> <li>• AG</li> <li>• Prosecutors</li> <li>• Law enforcement: state, county, city</li> </ul>				

Liability Issues				